

REMARKS

Claims 1-56 are pending in the present application. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 103, Obviousness

The Examiner rejected Claims 1-56 under 35 U.S.C. § 103 as being unpatentable over Jardin (6,681,327) in view of Matsumoto et al (cited by applicant on IDS 12/2/04). This rejection is respectfully traversed.

In the Examiner's response to Applicants arguments made in a Response to Office Action dated 3/21/05, the Examiner erroneously characterizes Applicants first argument as being a 'no suggestion to combine the references', and then states that the suggestion to combine references is in the knowledge generally available to one of ordinary skill in the art. This is an erroneously characterization – and thus the associated 'general knowledge rebuttal' is without merit – as Applicants argued that there would have been no motivation to combine the references. Specifically, there would have been no motivation to one of ordinary skill in the art to include an additional device such as Matsumoto's server to provide an encrypt/decrypt function to the teachings of Jardin, as Jardin already possesses processing blocks and associated functionality to perform encryption and decryption. In addition, Jardin requires that such encryption be performed directly by a broker server such that decrypted packets can easily be buffered and redirected to an intended recipient server (Jardin col. 2, line 56 – col. 3, line 3). Thus, a person of ordinary skill in the art would not have been motivated to combine Matsumoto's teachings with those of Jardin, as it would result in duplicate functionality (which is unnecessary and thus increases system cost and complexity), and would defeat an expressed desire by Jardin to perform encryption/decryption by the handshake broker itself. Therefore, the only motivation for combining the teachings of Matsumoto with the teachings of Jardin must therefore be coming from Applicants' own patent specification, which is *improper hindsight analysis*.

Still further with respect to the Examiner's response to Applicants arguments made in a Response to Office Action dated 3/21/05, the Examiner erroneously characterizes the teachings of the Matsumoto reference. The Examiner cites the Abstract

of Matsumoto as stating that a smart card can efficiently execute secret instructions (which Applicants do not object to), but the Examiner then states "Therefore, the auxiliary device executes secret computations (which Applicants do object to). The smart card and the auxiliary device as described by Matsumoto are *different devices*. The smart card is a client device and the auxiliary device is a server device (Matsumoto page 1, Section 1, second paragraph). The fact that the smart card (client device) executes secret instructions does not in any way establish that the auxiliary device (server device) executes secret instructions. Matsumoto expressly states that the auxiliary device is insecure (see, e.g., Matsumoto Title; Abstract). Matsumoto achieves the desired computational speed-up by offloading non-secret operations to the server, since it is an *untrusted server*¹. Thus, a person of ordinary skill in the art would have no motivation to combine Matsumoto's teaching of a smart card with an insecure server with the teachings of Jardin, as the resulting combination would be trying to perform encryption/decryption using an insecure server, which would defeat the entire purpose of using encryption/decryption as there would be no assurance that the insecure server could not be compromised. Thus, Applicants have further established that there would have been no motivation to combine the two cited references, as the resulting combination would not provide a *secured* encryption/decryption system since an *insecure* server (the auxiliary device) would be performing the encryption and decryption.

Still further with respect to Claim 1, because of Jardin's desire to use a common broker to provide *both* (i) handshake and decryption for a client (column 4, line 35 – column 6, line 3), *and* (ii) handshake and encryption for a back-end transaction server (column 7, lines 6-19), there would be no motivation to somehow separate the handshake and encryption/decryption functionality and still provide such dual-purpose functionality by a common broker, as expressly desired by the teachings of the cited Jardin reference – further evidencing no motivation to modify the teachings of Jardin in accordance with the claimed invention.

¹ Matsumoto teaches that he can use an insecure server in combination with his secret computational smart card by protecting the smart card's secrets from the server (page 2, line 6). This is accomplished by breaking up a secret algorithm to be performed into pieces, such that the client can perform the secret portion, and the server can perform non-secret portions (page 3, Section 3).

Even when the references have been improperly combined, Applicants show that there is still at least one missing claimed feature not taught or suggested by the cited references, further evidencing non-obviousness. In particular, none of the cited references teach or suggest utilizing one engine (an online crypto engine) to perform encryption or decryption *using cryptographic parameters established by another engine* (a handshake engine). In rejecting this aspect of Claim 1, the Examiner cites Matsumoto's server as teaching the claimed inline crypto engine, and Jardin's broker 120 as teaching the claimed handshake engine. Because these two devices (Matsumoto's server and Jardin's broker) are described in two separate references, it necessarily follows that there is no teaching or suggestion of the claimed co-action between such devices (as they are both described separately in their respective individual teachings, and thus there is no teaching of any synergistic co-action between these separately described devices), and in particular there is no teaching or suggesting of using parameters established by one of those devices (Jardin's broker) by the other of these devices (Matsumoto's server). Because Matsumoto's *server is insecure*, passing cryptographic parameters to such server would *compromise the encryption/decryption* of the overall system, thus evidencing that the resulting combination does not teach this missing claimed feature as such interpretation would result in a defective system.

Thus, even when the references have been improperly combined, there is still at least one missing claimed element, further evidencing non-obviousness. To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03 (emphasis added by Applicants); *see also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). In the absence of a proper *prima facie* case of obviousness, an applicant who complies with the other statutory requirements is entitled to a patent. *See In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).

The claimed co-action between the handshake engine and the inline crypto engine advantageously provides an ability to separate the handshaking functionality from the encryption/decryption functionality to improve performance, as the handshaking functionality is inherently much slower to perform (Specification page 13, lines 13-20). Per the present invention, this handshake functionality can be performed by a separate

handshake engine, thus offloading the handshake operations that would otherwise hinder the performance of the encryption/decryption engine (Specification page 14, lines 20-22).

Applicants initially traverse the rejection of Claims 2-18 and 48 for reasons given above regarding Claim 1 (of which Claims 2-18 and 48 depend upon).

Further with respect to Claim 4, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein the establishing step includes handing off a network connection from the transaction server to the handshake engine". In rejecting Claim 4, the Examiner cites Jardin's Figure 3 as teaching this claimed feature. Applicants urge that Jardin's Figure 3 describes the internal process flow between a broker 120 and a transaction server 130 (Jardin column 6, line 4 – column 7, line 56). Notably, it is Jardin's broker (which allegedly reads on the claimed handshake engine) that hands-off the communication link to a transaction server (Jardin, column 6, lines 39-41), which is just the opposite of what is recited in Claim 4, where the network connection is handed-off *from* the transaction server *to* the handshake engine. Quite simply, Jardin's transaction server does not have any type of network connection, and thus it does not have any network connection that can be handed off. In contrast, per Claim 4 (as depicted in the preferred embodiment in Applicants Figure 9) the transaction server itself has a network connection (as established by the process depicted in Figure 8 - note in particular the heavy line from the client/internet to the transaction server which bypasses the handshake engine), and thus has a network connection that is handed off to the handshake engine 900. This is not merely semantics, but a substantially different process and resulting data flow between the teachings of the cited references and the claimed invention as recited in Claim 4. Jardin teaches a network connection being made by a broker, with a back-end transaction server *which solely communicates with the broker via buffered storage* (col. 6, lines 9-12). Per Claim 4, the *transaction broker itself has a network connection*, and this network connection is handed off to the handshake engine (alleged to be Jardin's broker server). Thus, Claim 4 is further shown to not be obvious in view of the cited references.

With respect to Claims 16 and 17, Applicants previously amended such claims to specify that the inline crypto engine receives/transmits data from/to the network. In other words, the claimed inline crypto engine is located at the front-end of the system. In

contrast, Matsumoto's server (which is alleged to read on the claimed inline crypto engine) is a back-end processor. In rejecting Claim 16, the Examiner cites Jardin's part 430 of Figure 4 as teaching this claimed feature. Applicants urge that this further evidences the improper hindsight analysis being used by the Examiner in combining the references. Why would a person of ordinary skill in the art add a back-end crypto server (as alleged to be taught by Matsumoto) if the Jardin system being modified already has a front-end crypto server? Again, this duplication of functionality is unwieldy, costly, complex, and quite simply would make no sense to a person of ordinary skill in the art.

The Examiner is also impermissibly changing the interpretation of the cited references. In one instance, Matsumoto's server is being stated as teaching the claimed inline crypto engine (see page 4 of the present office action, where it states "Jardin does not disclose an inline crypto engine" in rejecting Claim 1), and yet the Examiner states in rejecting Claim 16 "Jardin discloses a system further comprising: receiving the transmitted data from the network by the inline crypto engine". If Jardin does not disclose an inline crypto engine (as admitted by the Examiner in the rejection of Claim 1), it necessarily follows that Jardin does not disclose receiving data from the network *by such missing inline crypto engine*. Thus, Claims 16 and 17 are further shown to not be obvious in view of the cited references, as there are further missing claimed features not taught or suggested by the cited references.

With respect to Claim 19 (and dependent Claims 20-37) and Claim 38 (and dependent Claims 39-47 and 49-56), Applicants traverse for similar reasons to those given above with respect to Claim 1.

Further with respect to Claims 22 and 41, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 4.

Further with respect to Claims 34 and 35, Applicants traverse for similar reasons to the further reasons given above with respect to Claims 16 and 17.

Further with respect to Claim 52, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein the at least one transaction server receives a request to establish the cryptographic parameters; and responsive to the at least one transaction server's receiving the request, the at least one handshake engine performs the establishing step". In rejecting Claim 52, the Examiner alleges that Jardin teaches the

features of Claim 52 at Jardin's Figure 2. Applicants urge that Jardin's Figure 2 is with respect to communication between a client 110 and a broker 120, and provides no teaching/suggestion of any transaction server, and in particular provides no teaching/suggestion of a transaction server that receives a request to establish the cryptographic parameters, as expressly recited in Claim 52. The Examiner has equated the claimed transaction server with Jardin's elements 130a, 130b and 130c of Figure 1 (per page 4 of the present Office Action, which cites Jardin col. 8, lines 5-17 as teaching the claimed transaction server). Neither this transaction server, nor its operations, is depicted in Jardin's Figure 2, and therefore the Examiner's citation of Jardin's Figure 2 as teaching the claimed transaction server features recited in Claim 52 is shown to be in error. Thus, Claim 52 is further shown to not be obvious in view of the cited references.

Still further with respect to Claim 52, it is urged that none of the cited references teach or suggest the claimed feature of "responsive to the at least one transaction server's receiving the request, the at least one handshake engine performs the establishing step". As can be seen, one server (transaction server) receives a request to establish cryptographic parameters, and another engine (handshake engine) actually establishes the cryptographic parameters responsive to the transaction server receiving the request. Jardin's Figure 2, which is being cited as teaching all features of Claim 52, merely shows a transaction between a client (which is not alleged to teach either the claimed transaction server or the handshake engine) and a broker (which is alleged to teach the claimed handshake engine, per page 4 of the present Office Action, citing Jardin column 4, lines 35-58). Thus, Jardin's Figure 2 does not depict or otherwise teach any type of transaction server, or co-action between a (missing) transaction server and handshake engine, as expressly recited in Claim 52. Thus, Claim 52 is further shown to have been erroneously rejected, as there are missing claimed features not taught or suggested by the cited references.

In summary, the Examiner's combination of references would result in a system having (1) duplicate/redundant functionality without purpose and (2) security compromises, thus evidencing an improper combination of references. Even with such improper combination, the synergistic co-action between the claimed handshake engine,

transaction server, and inline crypto engine is not taught or otherwise suggested, further evidencing non-obviousness of the present invention.

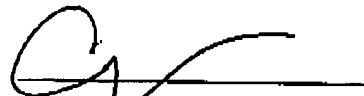
Therefore, the rejection of Claims 1-56 under 35 U.S.C. § 103 has been overcome.

II. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 8/3/05

Respectfully submitted,



Cathrine K. Kinslow
Reg. No. 51,886
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicant